Priemtesten

Frits Beukers

PWN Vakantiecursus voor wiskundeleraren 2023

Naïeve test

Is

$$N = 412068292467224099305295867294454137284725652929 61$$

priem?
Probeer alle (priem) getallen groter dan 1 en $< \sqrt{N} \approx 6 \cdot 10^{24}$ als deler.Stel dat 1 deling een nanoseconde duurt (10^{-9} seconde).
Maximale tijd:

$$6 \times 10^{24} \times 10^{-9} \text{ sec} = 6 \times 10^{15} \text{ sec} \approx 200.000.000 \text{ jaar.}$$

Geschatte looptijd van dit naïeve algorithme:
$C\sqrt{N} = C \exp(\frac{1}{2} \log N)$. We noemen dit een *exponentieel* algoritme.
Een algoritme heeft *polynomiale* looptijd als er $C, k > 0$ bestaan zó dat de looptijd kleiner is dan $C(\log N)^k$.

Toepassing stelling van Fermat

We weten, gegeven een getal n en a niet deelbaar door n:

$$n \text{ is priem } \Rightarrow a^{n-1} \equiv 1 (\mathrm{mod}\ n).$$

Neem contrapositieve,

$$n \text{ is niet priem } \Leftarrow a^{n-1} \not\equiv 1 (\mathrm{mod}\ n).$$

Pari opgave

Tik in: `n=2^127-1` en vervolgens

- `Mod(3,n)^k` voor een paar $k > 1000$, inclusief $k = n - 1$.
- `Mod(a,n)^(n-1)` voor een paar waarden van a.

Neem $n = 2^{67} - 1$ en bepaal $a^{n-1} (\mathrm{mod}\ n)$ voor een paar waarden van a. Wat zijn je conclusies?

Machtsverheffen mod n kan in lineaire tijd

Het is mogelijk om restklassen snel tot een hoge macht te verheffen.
Voorbeeld $a^{1111} \pmod{n}$ voor de een of andere a, n.

1. Schrijf de exponent $1111 = 2^{10} + 2^6 + 2^4 + 2^2 + 2 + 1$ (binaire schrijfwijze)
2. Bepaal achtereenvolgens $a^2 \pmod{n}, a^{2^2} \pmod{n}, \ldots, a^{2^{10}} \pmod{n}$ (herhaald kwadrateren).
3. Bepaal vervolgens het product $a^1 \cdot a^2 \cdot a^{2^2} \cdot a^{2^4} \cdot a^{2^6} \cdot a^{2^{10}} = a^{1111} \pmod{n}$.

In het algemeen willen we $a^k \pmod{n}$ bepalen. Aantal kwadrateringen is $< \log k / \log 2$. Aantal vermenigvuldigen is $< \log k / \log 2$.
Looptijd is $C \log k$.

Getuigen in de Fermat-test

De Fermat test is een *samengesteldheidstest* voor n. Een a, niet deelbaar door n, zó dat $a^{n-1} \not\equiv 1 (\mathrm{mod}\ n)$ noemen we een *getuige* van de samengesteldheid van n.
Helaas zijn er samengestelde getallen n die vrijwel geen getuige hebben.

Definitie

Een samengesteld getal n heet *Carmichael getal* als voor elke a met $\mathrm{ggd}(a, n) = 1$ geldt $a^{n-1} \equiv 1 (\mathrm{mod}\ n)$. Voorbeelden:
$n = 561, 1729, 294409, \ldots$

Stelling (Alford, Granville, Pomerance, 1992)

Er bestaan oneindig veel Carmichaelgetallen.

De Euler-test

We kunnen de stelling van Fermat iets verfijnen. Stel, a, n geheel en n oneven en geen deler van a. Dan geldt:

$$n \text{ priem} \Rightarrow a^{\frac{n-1}{2}} \equiv \pm 1 (\mathrm{mod}\ n).$$

Volgt direct uit het feit dat als n priem is, en dus $a^{n-1} - 1 = (a^{(n-1)/2)} - 1)(a^{(n-1)/2} + 1)$ deelt, hij één van de twee factoren deelt.
De contrapositieve uitspraak luidt

$$n \text{ samengesteld} \Leftarrow a^{\frac{n-1}{2}} \not\equiv \pm 1 (\mathrm{mod}\ n).$$

Deze samengesteldheidstest noemen we gemakshalve de *Euler-test*. Als n samengesteld is dan kan men aantonen dat minstens 50% van de restklassen $a(\mathrm{mod}\ n)$ daar onder de Euler-test getuige van is. Als voor veel verschillende a een 'positief' uitblijft, dan stijgt de kans dat n priem is. We spreken daarom van een *pseudo priemtest*.

Deterministische priemtest

Een bekende, en meest gebruikte, verfijning van de Euler-test is de zogenaamde *Rabin-test*.
Als het zogenaamde Gegeneraliseerde Riemann-vermoeden waar is, dan is er een getuige a voor de Rabin-test met $0 < a < 2(\log n)^2$ (Miller, 1976). Dat zou een deterministische polynomiale priemtest geven.
Vanaf 1985 zijn er diverse priemtesten (Cohen-Lenstra, Atkin-Morain) ontwikkeld waarmee men getallen tot enkele honderden cijfers deterministisch kon testen. Echter, geen van deze tests was aantoonbaar polynomiaal.

Een polynomiale priemtest

Stelling (Agrawal, Kayal, Saxena, 2002)

Er bestaat een polynomiale priemtest.

Input: geheel getal $n > 1$

1. Als $n = a^b$ voor $a \in \mathbb{N}$ en $b > 1$:
   output *Samengesteld*
2. Kies de kleinste $r \in \mathbb{N}$ zó dat $\mathrm{ord}_r(n) > 4(\log n)^2$.
3. Als $1 < \mathrm{ggd}(a, n) < n$ voor zekere $a \leq r$:
   output *Samengesteld*
4. Als $n \leq r$, output *Priem*
5. For $a = 1$ to $\lfloor 2\sqrt{r} \log n \rfloor$ do
   If $(X + a)^n \neq X^n + a (\mathrm{mod}\ X^r - 1, n)$:
   output *Samengesteld*
6. output *Priem*

Mersenne priemtest

Stelling (Lucas, 1876)

Stel $M_n = 2^n - 1$. Construeer de rij $S_1, S_2, S_3, \ldots$ modulo M_n door $S_1 = 4$ en $S_k = S_{k-1}^2 - 2$ voor $k \geq 2$. Dan,

$$M_n \text{ is priem} \Leftrightarrow S_{n-1} \equiv 0 (\mathrm{mod}\ M_n).$$

$n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203,$
$2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701,$
$23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433,$
$1257787, 1398269, 2976221, 3021377, 6972593, 13466917,$
$20996011, 24036583, 25964951, 30402457, 32582657,$
$37156667, 42643801, 43112609, 57885161, 74207281,$
$77232917, 82589933 (2018)$

Rep-units

Nauw verwant aan de Mersennegetallen zijn de zogenaamde rep-units,

$$\frac{10^n - 1}{9} = 1111 \cdots 11 \quad n \text{ enen.}$$

Het is bekend dat deze priem zijn voor
$n = 2, 19, 23, 317, 1031, 49081, 86453, \ldots$
In het algemeen bestaat $\frac{b^n-1}{b-1}$ uit enen in basis b. De Mersennegetallen zijn repunits in basis 2.

Rep-units zoeken

Pari opgave

Kies een geheel getal $g \geq 2$. Getallen van de vorm $\frac{g^n-1}{g-1}$ noemen we rep-units in basis g. We gaan er naar op zoek. Hiervoor kunnen we de PARI-opdracht isprime(n) gebruiken. Om type-werk te besparen definieren we eerst een zelfgemaakte functie.

```
rep(g)=for(n=2,50,if(isprime((g^n-1)/(g-1)),print(n)))
```

Geef vervolgens de opdracht `rep(10)`. Met de opdracht `rep(g)` wordt $\frac{g^n-1}{g-1}$ op primaliteit getest voor $n = 2, 3, ..., 50$. Je kunt 50 natuurlijk ook in een ander getal veranderen. Of de lus over priemexponenten laten lopen door `prime(n)` in plaats van `n` te gebruiken.